

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-232775**

(43)Date of publication of application : **27.08.1999**

(51)Int.Cl.

G11B 20/10

(21)Application number : **10-031846**

(71)Applicant : **MATSUSHITA ELECTRIC IND CO LTD**

(22)Date of filing : **13.02.1998**

(72)Inventor : **YAMADA MASAZUMI
IIZUKA HIROYUKI
TAKECHI HIDEAKI
GOTO SHOICHI**

(54) CONTROL STANDARD MAKING METHOD, CONTROL STANDARD MAKING SYSTEM, AND MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable detecting an illegal terminal device before damage occurs more surely than conventional one.

SOLUTION: When data is required from a VTR device 1030 and the like having respective intrinsic EU 164 to STB 120, a certification means 211 performs certification based on the prescribed control standard about their data request, it is decided whether required data is transferred from STB 120 to the VTR device 1030 performing request or not in accordance with the certification result, and a data request history information storing means 212 sends data request history information including EU 164 of the VTR device to a control device 110 in accordance with the certification result. The control device discriminates whether the VTR device 1030 is a regular one or not by the prescribed discrimination standard utilizing the data request history information, makes CRL based on the certification result, and sends it to the SBT 120.

* NOTICES *

JPO and INPIIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a criteria-of-control preparation method, a criteria-of-control preparing system, and a medium.

[0002]

[Description of the Prior Art] A receiver for exclusive use receiving, and recording the TV program etc. which are sent by satellite broadcasting with the VTR devices connected to the receiver, or viewing and listening to them on television conventionally, is performed.

[0003] In this case, what record is forbidden, and the conditional data whose record is enabled only once are in the image and voice data broadcast. Therefore, in order to keep these conditions, it will be the requisite that recognize this condition correctly and the user side uses the device which operates regularly.

[0004] Then, when transmitting data recordable once from a receiver for exclusive use, for example to VTR devices, usually authentication operation for checking first whether the VTR devices are the above regular devices is performed. Data is not transmitted when it judges with it being an inaccurate device which performs operation which disregarded the above-mentioned conditions as a result of this authentication operation.

[0005] Hereafter, it is explained as the composition of the conventional exclusive receiver and a terminal unit focusing on the authentication operation, referring to drawing 12.

[0006] Drawing 12 is a block diagram showing the conventional junction state and composition of an exclusive receiver and a terminal unit.

[0007] As shown in the figure, the antenna 1010 is a means to receive the broadcasting electric-wave from a satellite.

The satellite broadcasting receiver (this is only hereafter called STB) 1020 is a means to change the broadcasting electric-wave which received into AV information.

The data-communications line 1070 is a bus line for the data communications in which STB1020 and each terminal unit described below were formed in between. moreover -- a terminal unit -- ***** -- VTR devices -- (A) -- 1030 -- VTR devices -- (B) -- 1040 -- a recorder -- (C) -- 1050 -- furthermore -- TV -- a device -- (D) -- data communications -- a line -- 1070 -- STB -- 1020 -- connecting -- having -- **** .

[0008] Next, the internal configuration of STB1020 is described further, referring to the figure.

[0009] That is, the reception means 1021 is a means to link directly with the antenna 1010, to restore to the received data, to cancel the scramble for broadcast given to the received data, and to separate the multiplexed received data further. The encoding means 1022 is a means to encipher the AV information outputted from the reception means 1021 by the work key Kw for the encryption which it had beforehand with a compression state. The encoding means 1022 is a means for enciphering the work key Kw using the sub key obtained from the authentication means 1023, and outputting the enciphered work key and the both sides of the AV information which enciphered [above-mentioned] to a terminal unit via the data input/output means 1024. It is because it is premised on recording that it is necessary to also send here the work key enciphered as mentioned above to a terminal unit after decrypting the transmitted AV information in a terminal unit. The authentication means 1023 is a means to perform authentication work using a predetermined secret function, and to generate the sub key corresponding to an attestation partner as the result in order to confirm mutually whether each other's both devices are regular devices between

the terminal units which have carried out the transfer request of AV information. The authentication means 1023 makes all the peculiar secret functions (Sa, Sb, Sc, Sd, ..., Sn, ...) which all terminal units have correspond with those identification numbers, and holds them. The data transfer force means 1024 is IEEE1394 known as a digital interface. The data transfer means 1024 is a means to perform two transmission, isochronous transfer suitable for a data transfer like the image for which a real time nature guarantee is needed, or a sound, and asynchronous transfer suitable for transmission of data for attestation, a command, etc. without the necessity.

[0010]Next, the internal configuration of VTR devices (A) 1030 is described further.

[0011]The data transfer means 1031 is the same means as the data transfer means 1024 as shown in the figure.

It is a means to receive the enciphered work key and the enciphered AV information.

The authentication means 1032 has the peculiar secret function Sa beforehand.

It is a means to generate the sub key Ksa and to output to the decoding means 1033 as a result of authentication work.

The decoding means 1033 is a means to decrypt the enciphered work key which was obtained from the data transfer means 1031 by the sub key Ksa, and to decrypt the AV information which restored the work key Kw and was enciphered by the work key Kw. The record reproduction means 1034 is a means to record the decrypted AV information and to reproduce the record data.

[0012]In addition -- others -- a terminal unit -- it is -- VTR devices -- (B) -- 1040 -- a recorder -- (D) -- 1050 -- TV -- a device -- (D) -- 1060 -- a record reproduction means -- removing -- the above -- VTR devices -- (A) -- 1030 -- composition -- fundamental -- it is the same. However, the secret functions which each authentication means has beforehand will be Sb, Sc, and Sd, if it says in order of each above-mentioned device. Therefore, the sub keys generated by the authentication work of each device and STB1020 will be Ksb, Ksc, and Ksd, if it says in above order.

[0013]The contents of authentication work are described [in / next / the above composition] briefly.

[0014]For example, when performing the transfer request of AV information from VTR devices (A) 1030 to STB1020, in advance of the execution, the following authentication work is needed.

[0015]That is, first, the authentication means 1032 of VTR devices (A) 1030 generates the random number A1 and A2, and enciphers this with the secret function Sa. Here, the enciphered random number is indicated to be Sa (A1, A2). The authentication means 1032 transmits Sa (A1, A2) and the self identification number IDa to STB1020 via the data transfer means 1031 (Step 1001). Here, the identification number is beforehand given by the number peculiar to each terminal unit.

[0016]In STB1020, via the data transfer means 1024, the authentication means 1023 obtains Sa (A1, A2) and the identification number IDa, recognizes the identification number, and chooses the secret function Sa corresponding to it from two or more held secret functions (Step 1002). Thereby, the secret function which STB1020 should use for attestation between VTR devices (A) 1030 is specified.

[0017]Next, Sa (A1, A2) which the authentication means 1023 of STB1020 received [above-mentioned] using the secret function Sa is decoded, and the latter random number A2 is sent to VTR devices (A) 1030 among A1 restored and A2, without enciphering (Step 1003).

[0018]Next, the authentication means 1032 of VTR devices (A) 1030 compares A2 sent from STB1020 with the random number A2 which oneself generated at the above-mentioned step 1001. If both sides are in agreement, STB1020 can judge that it is a regular device (Step 1004).

[0019]Next, the authentication means 1023 by the side of STB1020 generates the random number B1 and B-2, and enciphers this with the secret function Sa. And Sa (B1, B-2) is transmitted to VTR devices (A) 1030 (Step 1005).

[0020]In VTR devices (A) 1030, Sa (B1, B-2) which the authentication means 1032 received [above-

mentioned] using the secret function Sa is decoded, and latter random number B-2 is sent to STB1020 among B1 and B-2s which were restored, without enciphering (Step 1006).

[0021]Next, the authentication means 1023 compares B-2 sent from VTR devices (A) 1030 with random number B-2 which oneself generated at the above-mentioned step 1005. If both sides are in agreement, it can be judged that VTR devices (A) 1030 are regular devices (Step 1007).

[0022]By the above, that both both sides are regular devices can check mutually, it comes, authentication work is completed, and transmission of the AV information to VTR devices (A) 1030 is permitted.

[0023]The four random numbers A1, A2, and B1 and B-2 exist in the authentication means 1023-1032 of both devices as a result of this authentication work. Then, next, both authentication means 1023-1032 generate the above-mentioned sub key Ksa using the random number A1 and B1, respectively. Since not using the random number A2 and B-2 has the circumstances where these were transmitted without enciphering, when generating a sub key, those who use the random number A1 without such the circumstances and B1 are because it sees from the safety of a key and excels more.

[0024]In the encoding means 1022, using the sub key Ksa generated by carrying out in this way, the work key Kw is enciphered and AV information is enciphered by the work key Kw. And the both sides of AV information Kw (AV) enciphered as the work key Ksa (Kw) enciphered [above-mentioned] are outputted to VTR devices (A) 1030 via the data input/output means 1024.

[0025]In VTR devices (A) 1030, the decoding means 1033 decodes the encryption work key Ksa (Kw) using the sub key Ksa obtained from the authentication means 1032, and decodes encryption AV information Kw (AV) using the decoded work key Kw.

[0026]

[Problem(s) to be Solved by the Invention]However, in the above authentication methods, an inaccurate person copies secret function Sn and the identification number IDn of a regular device as it is just as it is, When the inaccurate device which can perform the same authentication method as the above was manufactured and sold and the inaccurate device was used, in the above-mentioned authentication method, it has not detected that the device is an inaccurate device, and transmission of AV information was not able to be prevented.

[0027]Generally, in the unauthorized use by the 3rd person, such as a theft ATM card, direct damage occurs notably to the owner of the ATM card. Therefore, it is possible to prevent an unauthorized use promptly. On the other hand, as a receiving terminal device of broadcast data, even if the above inaccurate devices exist, there is peculiarity that damage to authorized personnel cannot surface easily. For example, even if it copies the data of copy prohibition unjustly, and it is rare that the concrete damage in which a royalty etc. are arrears surfaces and it surfaces, time most by it will have passed and it will also be expected that damage becomes serious.

[0028]Thus, in the conventional authentication method, since deer correspondence was not able to be performed after damage comes to light, it had the technical problem that it was imperfect as an authentication method.

[0029]An object of this invention is to provide the criteria-of-control preparation method, criteria-of-control preparing system, and medium which can ensure detection of an inaccurate device compared with the former in consideration of the technical problem of such a conventional method.

[0030]

[Means for Solving the Problem]When this invention according to claim 1 has a data request to a data transfer unit from each data request terminal unit which has a respectively peculiar identifier, about those data requests, As opposed to a data request terminal unit which performed attestation based on a predetermined attestation standard, and performed said data request from said data transfer unit according to a result of said attestation, Determine whether transmit the demanded data and a controlling device is

received from said data transfer unit according to a result of a usual state or said attestation, Send data request history information containing said identifier of the data request terminal unit, and said controlling device, It is a criteria-of-control preparation method which judges whether a data request terminal unit contained in the data request history information is regular, is based on the decision result, and creates or updates criteria of control by a predetermined judging standard using said data request history information sent.

[0031]This invention according to claim 5 a data transfer unit connected to each data request terminal unit which has a respectively peculiar identifier the singular number or a controlling device to manage [two or more], An identifier of a schedule connected newly or said data request terminal unit connected newly sent using new registration information to include by a predetermined judging standard. It is a criteria-of-control preparation method which judges whether a data request terminal unit corresponding to said new registration information is regular, is based on the decision result, and creates or updates criteria of control.

[0032]A criteria-of-control preparing system this invention according to claim 11 is characterized by that comprises the following.

Two or more data request terminal units which have a respectively peculiar identifier.

When a data request occurs from these data request terminal unit, about those data requests, performing attestation based on a predetermined attestation standard -- (1) -- to a data request terminal unit which performed said data request according to a result of the attestation, A data transfer unit which outputs data request history information which determines whether transmit the demanded data and contains said identifier of the data request terminal unit according to a result of (2) usual state or its attestation.

A controlling device which acquires said outputted data request history information, judges whether a data request terminal unit contained in the data request history information by predetermined judging standard is regular, is based on the decision result, and creates or updates criteria of control.

[0033]

[Embodiment of the Invention]Below, an embodiment of the invention is described with reference to drawings.

[0034](A 1st embodiment) Drawing 1 is a lineblock diagram showing the composition of the criteria-of-control preparing system in the 1 embodiment of this invention, and it describes the composition of the criteria-of-control preparing system of this embodiment, referring to the figure below. In this embodiment, the same numerals were given to what was explained by drawing 12, and the thing of the fundamentally same composition, and the detailed explanation was omitted.

[0035]As shown in drawing 1, the controlling device 110 is a device which manages the 1STB120 which exists in every place, ..., the nSTB130, and each terminal unit. The controlling device 110 is a means to create and distribute the inaccurate device list of [for each STB to use in authentication work]. The telephone line 140 is a means to use for the data communications between the controlling device 110 and each STB120,130. this embodiment -- 1st STB120 -- A Mr. house in Hokkaido -- the -- nSTB assumes that it is provided in N Mr. house in Okinawa.

[0036]The terminal unit is connected to each STB120,130 on the data-communications line 1070, respectively. That is, VTR devices 1030, VTR devices 1040, the recorder 1050, and the TV device 1060 are connected to the 1STB120, and VTR devices 150, the recorder 160, and the TV device 170 are connected to the nSTB130 as shown in the figure. Here, suppose that VTR devices 150 are inaccurate devices. This inaccurate device shall be a device manufactured by injustice by copying the thing of regular VTR devices 1030 as it is just as it is as the license key mentioned later and EUI64.

[0037]These each terminal unit is provided with IEEE1394 as the data transfer means 1031 as drawing 12.

explained it. In this embodiment, these terminal units are beforehand provided with EUI64 in IEEE1394 as a number peculiar to each device, i.e., an identification number, respectively. Here, EUI64 is a 64-bit identification code. These terminal units are provided with the license key corresponding to the identification number. Although this license key is a secret key given only to a regular terminal unit, the identification number of EUI64 is what is called an ID number that can be known also by whom on the occasion of data transfer etc. Hereafter, the identification number of EUI64 is only called EUI64 or an ID number. Peculiar EUI64 is provided also about each STB120,130. To each device, these identification numbers support the couple 1 and do not overlap.

[0038]Next, the internal configuration of STB120 is described in detail, referring to drawing 2.

[0039]In addition to the composition of the authentication means 1023 described by drawing 12, STB120 is provided with the data request history information storage means 212, the modem 213, the CRL recording device 214, and the CRL storing means 215 as shown in drawing 2.

[0040]The authentication means 211 are a point provided with the service key formation function which can make the service key which is the same key as a license key, and a point which takes into consideration the list of the inaccurate device mentioned later in attestation, and are different from the authentication means 1023 described by drawing 12. This service key formation function is a function which generates a service key from EUI64 (ID number) obtained from the terminal unit. Therefore, the authentication means 211 does not need to memorize EUI64 of a terminal unit beforehand.

[0041]The data request history information storage means 212 is a means to generate the hysteresis information about the data request, and to memorize through the authentication work mentioned later each time about what transmission of requested data completed, when the data transfer request of a predetermined program occurs from a terminal unit. This data request history information comprises EUI64 of the terminal unit which carried out the data transfer request, time information which specifies time with the data request from that terminal unit, and location information which specifies the whereabouts of that terminal unit. The data request history information storage means 212 acquires these EUI(s) information - location information from the authentication means 211. The data request history information storage means 212 accumulates such hysteresis information from each terminal unit of one-month Hazama, and is a means sent to the controlling device 110 via the modem 213 for every month.

[0042]The CRL recording device 214 is a means which obtains the list data for which the inaccurate device sent from the controlling device 110 was indicated from the modem 213, and is recorded and updated at the CRL storing means 215. The CRL storing means 215 is a memory means for storing the list data of an inaccurate device. In this specification, the list of an inaccurate device is only called CRL (Certification Revocation List). The criteria of control of this invention according to claim 1 correspond to CRL.

[0043]Next, the internal configuration of the controlling device 110 is described in detail, referring to drawing 3.

[0044]The history information storage means 112 is a means to make each data request history information transmitted for every month from each STB120,130 at the period correspond with EUI64 of STB of a transmitting agency, and to memorize it temporarily via the modem 111 as shown in drawing 3. The unjust device determining means 113 in all the data request history information for one month from each STB memorized by the above-mentioned history information storage means 112, When two or more EUI64 [same] exist, it is a means to determine the data request terminal unit which compares the time information and location information corresponding to EUI64 of these plurality, respectively, and has EUI64 with an unjust possibility. The CRL preparing means 114 is a means to obtain the above-mentioned decision results outputted for every month from the unjust device determining means 113, to create the list of an inaccurate device, and to output. All the CRL memory measures 115 are means to obtain the list data

from the CRL preparing means 114, to make addition of a new inaccurate device, correction of data, etc. to the already accumulated list, and to memorize all the CRL(s) about the terminal unit of all the areas. The individual CRL preparing means 116 is a means to transmit to STB which creates individual CRL corresponding to each STB, and corresponds via the modem 111. Individual CRL is a list of the inaccurate device packed for every STB, and is not created about STB from which the inaccurate device is not detected.

[0045]Mainly referring to drawing 4 - drawing 6 (c), operation of this embodiment is described and the 1 embodiment which starts the criteria-of-control preparation method of this invention simultaneously is also described [in / next / the above composition]. Drawing 4 is a figure to explain the memory content of the data request history information storage means 212 in STB120 from January 1, 1997 to the 31st of the same month, and drawing 5. It is a figure explaining the memory content of the history information storage means 112 in the controlling devices from January 1, 1997 to the 31st of the same month.

[0046]Here, as of January 31, 1997, to CRL (list of an inaccurate device) of the CRL storing means 215 of STB120, the inaccurate device is not yet indicated, i.e., it presupposes at it that it is in an empty situation. It is sky condition also about CRL of the CRL storing means of STB130.

[0047]First, explanation here describes the authentication operation using CRL in (1) STB, next describes creation of CRL in (2) controlling devices, and distribution of CRL to STB, and states the updating operation of CRL in (3) STB to the last.

(1) Authentication operation using CRL in STB : here, when STB120 receives the transfer request from VTR devices 1030 which are regular devices about the AV information of the program which received by the reception means 1021, for example, perform the following authentication operation. This transfer request satisfies the demand which suited at 12:10 a.m. on January 10, Heisei 10 in the hysteresis information indicated in drawing 4 and drawing 5.

[0048]Step 1: The authentication means 211 of STB120 obtains first EUI64 (here, they may be No. 11030) of VTR devices 1030 which have carried out the transfer request from the data transfer means 1024.

[0049]Step 2: and the authentication means 211 confirm whether the same number as the EUI64 is registered in CRL as a number of an inaccurate device with reference to CRL of the CRL storing means 215. At this time, since CRL is sky condition as above-mentioned, the decision result of being unregistered comes out and that EUI64 goes into full-scale authentication work (Step 3). If a judgment that it registers with CRL comes out in this check stage, subsequent authentication work will not be performed and a data transfer with a demand will not be performed, either.

[0050]Step 3: The authentication means 211 generates a service key from a service key formation function using EUI64 of VTR devices 1030 obtained at Step 1. Thus, the generated service key is the same key as the license key which VTR devices 1030 have. A license and a service key correspond to the secret function Sa described by drawing 12.

[0051]On the other hand, VTR devices 1030 perform the same authentication work as what was already explained by drawing 12 by both Hazama using the license key which it has beforehand using the service key which carried out the authentication means 211 in this way, and was generated. That is, both devices generate the same sub key Ksa using the random number A1 and B1, respectively.

[0052]Step 4: The encoding means 1022 enciphers the work key Kw using the above-mentioned sub key Ksa, and enciphers AV information using the work key Kw, and transmits the encryption data (Ksa (Kw), Kw (AV)) of these both sides to VTR devices 1030.

[0053]Supposing it is a process of this attestation and EUI64 sent from the terminal unit is a completely random number which does not have the correspondence relation beforehand determined as the license key which that terminal unit has, for example, The key generated by the service key formation function

stops being in agreement with the license key. because, a service key formation function -- the account of the upper -- it is because it is constituted based on the correspondence relation defined beforehand so that a service key may be generated from EUI64. Therefore, the data transfer which the above-mentioned attestation on condition of the key which both devices have in this case being the same stops having materialized, and was demanded in this case is not performed.

[0054]Step 5 : the data request history information storage means 212, From the authentication means 211 as EUI64 of VTR devices 1030 which are the destination about what data transfer completed at Step 4, As No. 11030 and time information with a demand, each information at 12:10 a.m. on January 10, Heisei 10 is acquired, and it records as data request history information (refer to drawing 4). Here, the statement of drawing 4 is explained. Namely, No. 31060 as each number written in the column 401 of EUI64 of a terminal unit in the figure, No. 11040, No. 11030, and No. 21050, Sequentially from before, EUI64 of the TV device 1060, VTR devices 1040, VTR devices 1030, and the recorder 1050 is shown.

[0055]Step 6: Whenever a data transfer request occurs from each terminal units 1030-1060, perform the above-mentioned steps 1-5 like the above. And the data request history information storage means 212, To each historical data (refer to drawing 4) by which record accumulation was carried out in one month, it is EUI64 (here) of STB120. And you consider it as No. 90001, let what attached the telephone number as the location information be data request history information (it transmits to the controlling device 110 for every month via the telephone line 140 from the modem 213.).

(2) Creation of CRL in a controlling device, and distribution operation of CRL to STB : here, describe operation of the controlling device 110.

[0056]Step 101: The data request history information mentioned above for every month is transmitted to the history information storage means 112 of the controlling device 110 via the modem 111 from STBs 120-130 of every place. The history information storage means 112 holds these information as hysteresis information.

[0057]Step 102: The unjust device determining means 113 acquires the hysteresis information held at the history information storage means 112, and rearranges a data content into time order by the time information (refer to drawing 5). Drawing 5 is a figure for explaining the contents of the rearranged hysteresis information.

[0058]And if there is what has EUI64 [same] of the terminal unit shown in the column 501 (refer to drawing 5) of EUI64 of a terminal unit, the time information and location information corresponding to them will be compared, respectively, and the terminal unit corresponding to EUI64 with an unjust possibility will be determined.

[0059]That is, when shown in drawing 5, all EUI64 of the terminal unit indicated in each line to which the numerals 511,512,513 were given are No. 11030. Then, these are checked first. When the time information of the line to which the numerals 511 and 512 were given is compared, it is a history of the transfer request in time different, respectively, and it can be judged that there is no inconsistency in both histories. However, it is shown that the situation which is contradictory to the premise of not existing has generated the device which has EUI64 with two same histories indicated in the line which attached the numerals 512 and 513. The number 90002 written in the column 504 of EUI64 of STB of drawing 5 is EUI64 of STB130.

[0060]Namely, when the unjust device determining means 113 compares the data of the column 502 of the time information of these both sides, and the column 503 of location information, it is a 10-minute [after the place where one side calls it Okinawa and another side is called Hokkaido and which was left distantly geographically] difference, It sees from the fact that there was a transfer request with the device which has the EUI64 [same], and the device which has the EUI64 [same] judges that it exists in A Mr. house in Hokkaido, and N Mr. house in Okinawa. And the both sides of the device of these both sides consider

that the unjust device determining means 113 is an inaccurate device, and it sends the decision result to the CRL preparing means 114. Although VTR devices 150 currently installed in N Mr. house in Okinawa are actually inaccurate devices, since it does not understand, in this stage, it considers that both sides are inaccurate for the time being till the place which says any are actually inaccurate devices. That judgment with unjust any is mentioned later. The situation which is contradictory to the premise that the device which has the EUI64 [same] from the result of having compared the historical data indicated in the line which attached the numerals 521,522 does not exist is not found.

[0061]Step 103: From the decision result obtained from the unjust device determining means 113, the CRL preparing means 114 creates CRL as shown in drawing 6 (a), and sends it to all the CRL memory measures 115. Such creation operation of CRL is performed every month, and it memorizes at all the CRL memory measures 115 at every time. Therefore, with the list sent from the CRL preparing means 114, all the CRL memory measures 115 add an addition, correction, etc. to already memorized CRL, and update them each time.

[0062]Step 104: The individual CRL preparing means 116 separates the contents of the CRL for every STB, seeing the column 601 of EUI64 of STB in CRL created by the CRL preparing means 114. Drawing 6 (b) and (c) is individual CRL created, respectively in order to distribute to STB130 and STB120. The individual CRL preparing means 116 distributes these individual lists to corresponding STB via the modem 111.

(3) Updating operation of CRL in STB : STB120 which obtained individual CRL (refer to drawing 6 (c)) distributed from the controlling device 110 performs the following operations.

[0063]Step 201:214, i.e., a CRL recording device, obtains the above-mentioned individual CRL from the modem 213, and it records it on the CRL storing means 215 which was sky condition till then. Thereby, connection, now VTR devices 1030 (EUI64 is No. 11030) which are registered into the CRL storing means 215 by STB120 as an inaccurate device. Therefore, since it becomes clear in the stage of the above-mentioned step 2 that it is an inaccurate device even if the data transfer request from these VTR devices 1030 will occur from now on, there is no data transfer limping gait *****. Thereby, expansion of the damage caused by an inaccurate device can be prevented. Also in STB130, same operation is completely performed. In this case, VTR devices 150 (EUI64 is No. 11030) are registered into the CRL storing means of STB130 as an inaccurate device.

[0064](A 2nd embodiment) Drawing 7 and 8 are the lineblock diagrams showing the composition of STB and the controlling device which constitute the criteria-of-control preparing system in the 1 embodiment of this invention, and they describe the composition of the criteria-of-control preparing system of this embodiment, referring to the figure below. In this embodiment, the same numerals were given to what was explained by a 1st embodiment, and the thing of the fundamentally same composition, and the detailed explanation was omitted. The composition of the whole system of this embodiment is the same as what was fundamentally described by drawing 1.

[0065]The main points of difference between this embodiment and the above-mentioned embodiment are the processes of creation of the injustice and regular determination information about a terminal unit. Therefore, it explains focusing on this point of difference here. The criteria of control of this invention according to claim 5 correspond to injustice and regular determination information.

[0066]The main points which are different from the composition shown by drawing 2 in the composition of STB120 shown in drawing 7, The new contact detection means 711, injustice and a regular information storing means 712, and injustice and a regular information storage means 713 are provided instead of the data request history information storage means 212 of drawing 2, the CRL storing means 215, and the CRL recording device 214. Unlike what was described by a 1st embodiment, the authentication means 714 does not have composition which outputs the hysteresis information about the data transfer request from a

terminal unit. Other composition is the same.

[0067]The new contact detection means 711 is a means to detect it and to acquire the EUI64, when there is a device newly connected to the data-communications line 1070 of STB120. EUI64 acquired attaches EUI64 of STB120 and is sent to the controlling device 110 from the modem 213. This operation is the work for the new registration to the controlling device of the newly connected device, and is also the work for checking simultaneously whether that new contact is inaccurate. Since this operation is performed in the case of new registration, unlike what is performed to the degree of the data transfer request described by a 1st embodiment of the above, it is first-time operation.

[0068]Injustice and the regular information storage means 713 are means to store in injustice and the regular information storing means 712 the information sent from the controlling device 110.

[0069]Next, the composition of the controlling device 110 is described, referring to drawing 8.

[0070]As shown in the figure, the inquiry means 811 obtains EUI64 of the terminal unit which is sent from STBs 120-130 and which was newly established as new registration information, and EUI64 of STB of the transmitting origin, and is a means to judge whether it is inaccurate. The new registration device list information memory measure 812 is a means to memorize EUI64 of the new registration device obtained from the inquiry means 811.

[0071]Injustice and the regular determination information preparing means 813 are means to create whether to be inaccurate and that regular determination information about the device which had new registration from the above-mentioned checked result by the inquiry means 811, and to transmit which the information to corresponding STB via the modem 111. When it becomes double registrations, injustice and the regular determination information preparing means 813 consider that the device of the both sides which have the EUI64 is an inaccurate device, and creates and distributes the list corresponding for every STB of unjust information (refer to drawing 6 (b) and (c)).

[0072]Mainly referring to drawing 9 (a) - drawing 10 (b), operation of this embodiment is described and the 1 embodiment which starts the criteria-of-control preparation method of this invention simultaneously is also described [in / next / the above composition]. VTR devices 1040 shown in drawing 1 by this embodiment on account of explanation, the recorder 1050, and the TV device 1060, finishing [connection with STB120] already -- it is -- finishing [VTR devices 150, the recorder 160, and the TV device 170 / connection with STB130] already -- it is -- it is assumed that ** and the new registration explained below have also ended just to these terminal units. VTR devices 1030 presuppose that it is a device newly connected to STB120. VTR devices 150 presuppose that it is an inaccurate device as the above-mentioned embodiment also explained them. Explanation here describes first the detecting operation of the device connected newly in (1) STB, Next, the authentication operation which used the renewal of injustice and regular determination information, and the injustice and regular determination information in (3) STB for the last about creation of the new registration, and the injustice and regular determination information in (2) controlling devices, etc. is described. These explanation is given focusing on a point of difference with a 1st embodiment.

(1) Operation in STB : suppose that VTR devices 1030 were newly connected to STB120 as above-mentioned (refer to drawing 7).

[0073]Step 201: The new contact detection means 711 shown in drawing 7 reads periodically EUI64 of all the terminal units connected to the data-communications line 1070, and records it on the memory (graphic display abbreviation) to build in. And it compares with the newest record data of EUI64 of the terminal unit already recorded.

[0074]In the situation where VTR devices 1030 were newly connected, the periodical thing of above-mentioned EUI64 it read and the device of No. 11030 was newly connected [the thing] for EUI64 by the above-mentioned comparison operations is detectable.

[0075]Step 202: The new contact detection means 711 transmits to the controlling device 110 via the modem 213 further by making into new registration information EUI64 (No. 11030) of the device which is the target of the new registration detected [above-mentioned], and EUI64 (No. 90120) of STB120 of a transmitting agency.

(2) Operation in a controlling device : drawing 9 (a) is a figure for explaining the memory content of the new registration device list information memory measure 812 before registering VTR devices 1030, and drawing 9 (b) is the figure after VTR devices 1030 were registered. It explains referring to these drawings.

[0076]Step 301: Based on the new registration information transmitted from SBT120, the inquiry means 811 shown in drawing 8 investigates the memory content (refer to drawing 9 (a)) of the new registration device list information memory measure 812, and confirms whether the registration produces the situation of double registrations. EUI64 contained in new registration information is No. 11030, and this already overlaps with a registered thing (the numerals 901 were attached among drawing 9 (a)) as it shows drawing 9 (a). Therefore, about EUI64 of the duplicate both sides, the inquiry means 811 judges with it being inaccurate, and outputs.

[0077]Step 302: The new registration device list information memory measure 812 registers the contents of the new registration information sent from the inquiry means 811 (the numerals 902 were attached among the figure).The information on an unjust purport is recorded on the remarks column 903 about EUI64 of the duplicate both sides from the above-mentioned decision result. The judgment of any are really inaccurate is mentioned later.

[0078]Step 303: Injustice and the regular determination information preparing means 813 create the list of injustice and regular determination information as shown in drawing 10 (a) and (b) from the decision result sent from the inquiry means 811. These lists are packed for every STB. The information which shows injustice is recorded on the column 101 of the decision result by drawing 10 (a) and (b) as above-mentioned. However, when judged with it being regular as a result of the judgment of the new registration information by the inquiry means 811 in Step 301, the information which shows a norm needless to say is recorded on the column 101 of a decision result.

[0079]Step 304: Injustice and the regular determination information preparing means 803 transmit the individual list of decision results created as mentioned above to STB120 and STB130 via the modem 111. This transmission is performed whenever the new registration information mentioned above is sent from STB.

[0080](3) Operation in STB : drawing 11 (a) is a figure showing the contents already stored in injustice and the regular information storing means 712, and shows the situation before transmitting the individual list of decision results shown in drawing 10 (a). Drawing 11 (b) shows the situation after the contents of the individual list of decision results shown in drawing 10 (a) were reflected.

[0081]The injustice and the regular information storage means 713 shown in drawing 7 obtain the individual list of decision results transmitted from the controlling device 110 from the modem 213, and adds it to the contents of record shown in drawing 11 (a). The contents of the above-mentioned individual list are added to the 4th line (the numerals 1113 were attached among the figure) from on drawing 11 (b). The column 1111 of the decision result of the figure shows whether the device shown in the column 1112 of EUI64 of a registering terminal device is inaccurate or regular.

[0082]On the other hand, also in STB130, the completely same operation as the above is performed.

[0083]Next, the case where there is a transfer request of AV information is described from VTR devices 1030 to STB120.

[0084]In this case, in the authentication operation described at Step 1 described by a 1st embodiment - Step 4, since only the contents of the above-mentioned step 2 differ, only that point of difference is described.

[0085]That is, the authentication means 714 confirms whether EUI64 of the terminal unit which advanced the transfer request is regular or inaccurate with reference to injustice and the regular information storing means 712 after the same operation as the above-mentioned step 1. According to the information recorded on the line which attached the numerals 1113, it is shown that EUI64 which has carried out the above-mentioned transfer request is unjust as for the device of No. 11030 as shown in drawing 11 (b). Therefore, the authentication means 714 does not perform subsequent authentication work, and does not perform a data transfer with a demand, either.

[0086]As a result of a check, when regular, the same operation as the contents described at the above-mentioned steps 3-4 is performed.

[0087]When EUI64 of a device with a transfer request is unregistered to injustice and the regular information storing means 712, it directs that the authentication means 714 sends the new registration information on the device of the demand origin to the controlling device 110 to the new contact detection means 711. Thereby, expansion of the damage caused by an inaccurate device can be prevented.

[0088]By the way, it is **** about the judgment of the any when it is judged with both devices being inaccurate as mentioned above, are really inaccurate.

[0089]In this case, since the user who did not have the data which it was considered by STB that it was inaccurate and was demanded transmitted tumefies doubt of the device which received that unjust judging, he can request investigation from the control center which owns the controlling device 110. The control center which received the investigation request investigates the truth of the device, and confirms certainly whether be what was manufactured or converted by the inaccurate method. And if it turns out to be regular, the data currently recorded on the controlling device will be corrected and the correcting result will be transmitted to applicable STB. A transfer request will be accepted to the device which turned out to be regular by this.

[0090]A magnetic recording medium, an optical recording medium, etc. which recorded the program for making a computer perform any of the embodiment described above or all or a part of steps (MEANS) of each steps (or means) of one statement can be created, and the same operation as the above can also be performed using this. The same effect as the above is demonstrated also in this case.

[0091]Although the above-mentioned embodiment described the case where it recorded on the data request history information storage means 212 for all the data transfer requests which occurred from the terminal unit, the composition recorded only for the transfer request of not only this but data important for example, may be used. Here, it is paper Lec (PREC) and data like pay-per-view (PPV) of charging as important data, for example if it records. Therefore, what pays money for every chain flannel, for example, the program data of a free channel, etc. are good also as outside of an object.

[0092]Although a 2nd embodiment of the above described the case where it was detected automatically that the terminal unit was newly connected, the registration postcard is attached not only to this but to the device purchased newly, for example, and it is good also as composition with which a user sends the postcard to the control center which owns a controlling device.

[0093]Although the above-mentioned embodiment described the case where transmission to STB of CRL, or injustice and regular information was performed using a telephone line, it may send not only by this but by broadcast.

[0094]Although a 2nd embodiment of the above compared the new registration information sent from the STB side, and the already sent accumulation data of new registration information and described the case where it checked for no duplication, It may have a memory holding the list data of EUI64 of a produced regular device indicated to the production information led from each company which manufactured not only this but the device, and the composition of also performing comparison with the contents of the memory may be used in the case of the above-mentioned comparison. Even when EUI64 contained in new

registration information is completely random, by comparing with the contents of the above-mentioned memory, If it is a number which does not correspond, it is not recorded on the new registration device list information memory measure 812 even if, but even if it is in the situation not overlapping, it can judge with it being inaccurate and the effect of dishonesty prevention will improve more.

[0095]The above-mentioned embodiment is available even for even referring to not only this but only referring to CRL as for example, contents of attestation, or injustice and regular information, although the case where full-scale authentication operation was performed was described.

[0096]Using a computer, work of a program may realize by software or the processing operation of each means of the above-mentioned embodiment may realize the above-mentioned processing operation in hard by circuitry characteristic for not using a computer.

[0097]The data transfer unit of the invention in this application was STB in the above-mentioned embodiment, when the STB detected connection with STB of the data request terminal unit connected newly, it explained the case where the new registration information on the data request device was transmitted to a controlling device, but. Not only in this, for example, the new contact detection means 711, If there is nothing same as compared with EUI64 of the terminal unit which obtains EUI64 of the VTR devices 1030, already checks new connection, and is recorded when attestation is newly required from VTR devices 1030, The composition detected as what was connected newly may be sufficient as the VTR devices 1030.

[0098]By the above-mentioned embodiment, when it has been checked as a result of attestation that it is a regular device, explained the example of sending the data request history information which contains the identifier (EUI64) of the data request terminal unit from a data transfer unit (STB) to a controlling device, but. It may not be concerned with the result of not only this but attestation, but the composition of sending the data request history information may be used to a controlling device. In this case, what is necessary is just to send with hysteresis information also that, when it becomes clear that it is an inaccurate device in process of attestation.

[0099]Although the above-mentioned embodiment described the case where STB used the criteria of control (CRL, or injustice and regular determination information) of the invention in this application in authentication operation, the composition which uses neither the above CRL, nor injustice and regular determination information in the authentication operation not only as this but as an STB may be used.

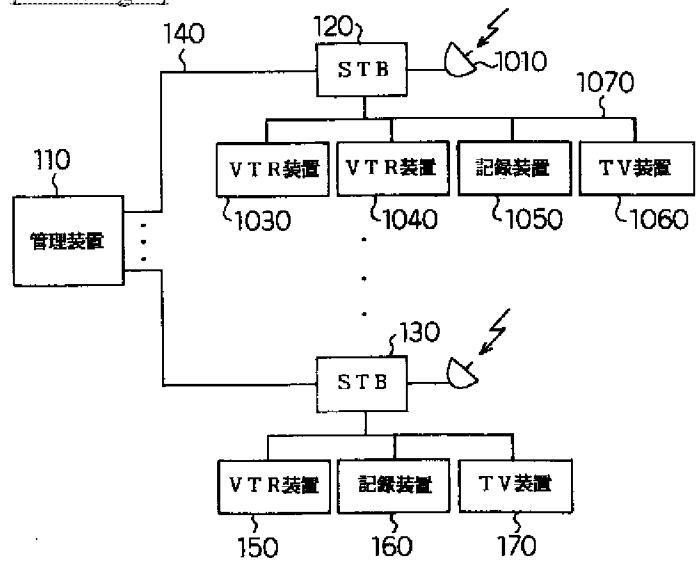
[0100]

[Effect of the Invention]This invention has the strong point in which detection of an inaccurate device can be ensured compared with the former so that clearly from the place described above.

[Translation done.]

DRAWINGS

[Drawing 1]

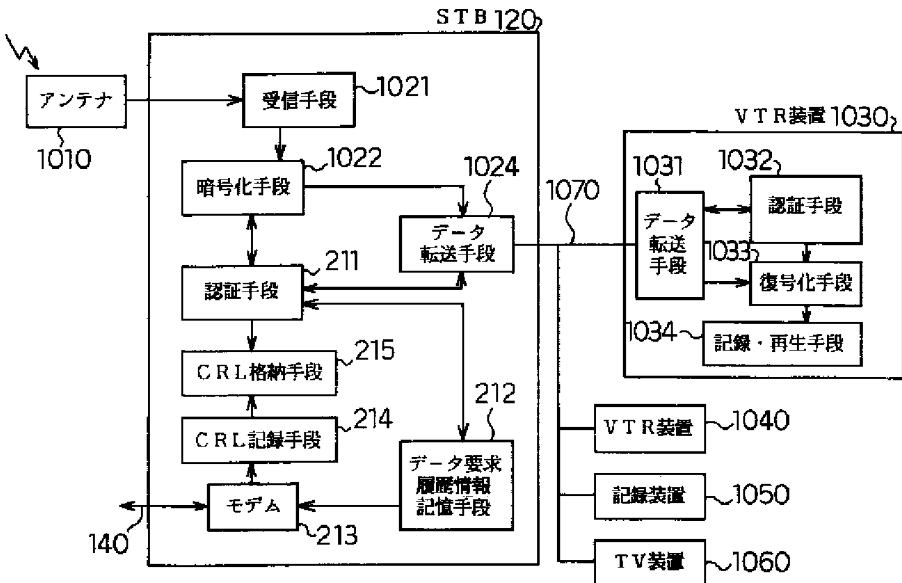


[Drawing 4]

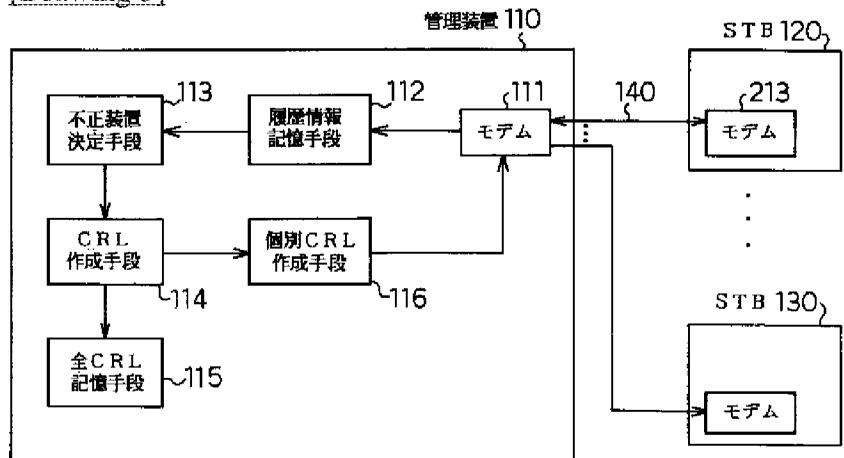
401

端末装置のEUI 64	時刻情報
31060	1998年1月 1日 12:00
11040	1998年1月 1日 15:00
:	:
11030	1998年1月 10日 12:10
:	:
11040	1998年1月 30日 7:00
21050	1998年1月 31日 23:00

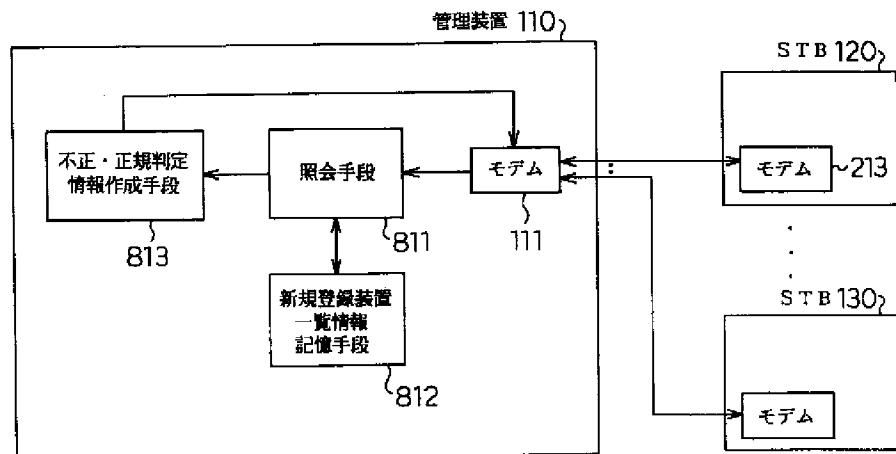
[Drawing 2]



[Drawing 3]



[Drawing 8]



[Drawing 5]

	501	502	503	504
	端末装置のEUI64	時刻情報	所在情報	STBのEUI64
511~	11030 31060	1998年1月 1日11:00 1998年1月 1日12:00	沖縄のNさん宅の電話番号 北海道のAさん宅の電話番号	90130 90120
521~	11040	1998年1月 1日15:00	北海道のAさん宅の電話番号	90120
	:	:	:	:
512~	11030	1998年1月10日12:00	沖縄のNさん宅の電話番号	90130
513~	11030	1998年1月10日12:10	北海道のAさん宅の電話番号	90120
	:	:	:	:
	20160	1998年1月30日10:00	沖縄のNさん宅の電話番号	90130
522~	11040 21050	1998年1月30日 7:00 1998年1月31日23:00	北海道のAさん宅の電話番号 北海道のAさん宅の電話番号	90120 90120

[Drawing 6]

(a)

601	
端末装置のEUI64	STBのEUI64
11030	90130
11030	90120

(b)

端末装置のEUI64	STBのEUI64
11030	90130

(c)

端末装置のEUI64	STBのEUI64
11030	90120

[Drawing 9]

(a)

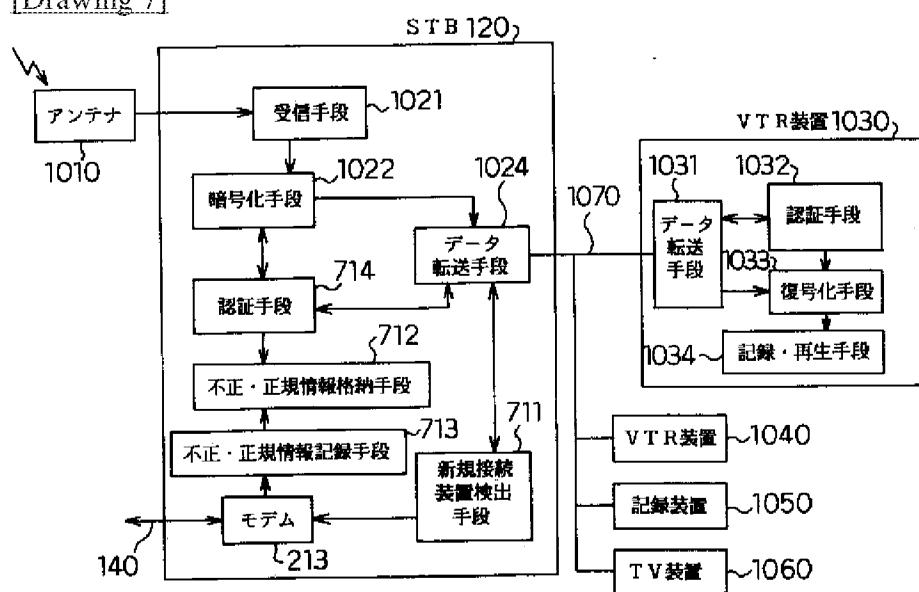
登録端末装置の EUI64	STBの EUI64	備考
11030	90130	
31060	90120	
11040	90120	
21050	90120	
20160	90130	
30170	90130	

(b)

903

登録端末装置の EUI64	STBの EUI64	備考
11030	90130	不正
31060	90120	
11040	90120	
21050	90120	
20160	90130	
30170	90130	
11030	90120	不正

[Drawing 7]



[Drawing 10]

(a)

101		
登録端末装置の EUI64	STBの EUI64	判定結果
11030	90130	不正

(b)

登録端末装置の EUI64	STBの EUI64	判定結果
11030	90120	不正

[Drawing 11]

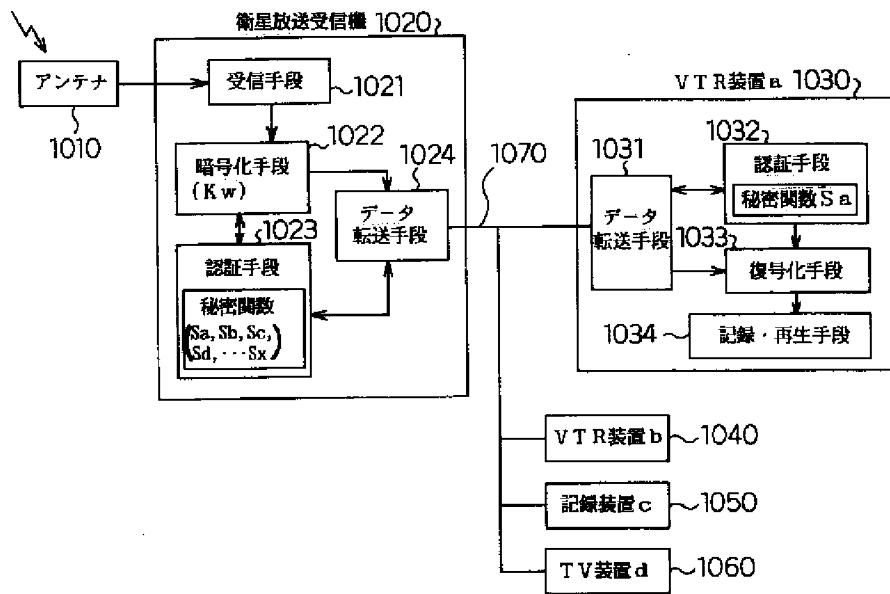
(a)

登録端末装置の EUI64	判定結果
31060	正規
11040	正規
21050	正規

(b)

登録端末装置の EUI64	判定結果
31060	正規
11040	正規
21050	正規
11030	不正

[Drawing 12]



[Translation done.]

CLAIMS

[Claim(s)]

[Claim 1]When a data request occurs to a data transfer unit from each data request terminal unit which has a respectively peculiar identifier, about those data requests, As opposed to a data request terminal unit which performed attestation based on a predetermined attestation standard, and performed said data request from said data transfer unit according to a result of said attestation, Determine whether transmit the demanded data and a controlling device is received from said data transfer unit according to a result of a usual state or said attestation, Send data request history information containing said identifier of the data request terminal unit, and said controlling device, A criteria-of-control preparation method judging whether a data request terminal unit contained in the data request history information is regular, being based on the decision result, and creating or updating criteria of control by a predetermined judging standard using said data request history information sent.

[Claim 2]Are information characterized by comprising the following and said predetermined judging standard in said controlling device, In all the data request history information transmitted from said two or more data transfer units, The criteria-of-control preparation method according to claim 1 being what determines a data request terminal unit which compares said time information corresponding to an identifier and said location information of these plurality, respectively, and has an identifier with an unjust possibility when two or more same identifiers exist.

Time information which specifies time with said data request from said data request terminal unit with which a group formed by a data request terminal unit and said data transfer unit of said plurality has those with two or more groups, and said data request history information has the identifier other than said identifier.

Location information which specifies the whereabouts of the data request terminal unit.

[Claim 3]When a data request terminal unit which has an identifier with a decision result by said judging standard and said unjust possibility is determined, consider that all the data request terminal units which have the identifier same in them are inaccurate things, and as said criteria of control, The criteria-of-control preparation method according to claim 2 creating or updating an unjust list of data request terminal units it was considered that were these inaccurate things.

[Claim 4]The criteria-of-control preparation method according to claim 3, wherein said controlling device transmits said all or some of unjust list to said data transfer unit and said data transfer unit performs said attestation, using said transmitted unjust list at least.

[Claim 5]A data transfer unit connected to each data request terminal unit which has a respectively peculiar identifier the singular number or a controlling device to manage [two or more], An identifier of a schedule connected newly or said data request terminal unit connected newly sent using new registration information to include by a predetermined judging standard. A criteria-of-control preparation method judging whether a data request terminal unit corresponding to said new registration information is regular, being based on the decision result, and creating or updating criteria of control.

[Claim 6]A group formed by a data request terminal unit and said data transfer unit of said plurality those with two or more groups, and said data transfer unit, When connection with said data transfer unit of said data request terminal unit connected newly is detected, Transmit new registration information on the data request device to said controlling device, and said predetermined judging standard, The same identifier as an identifier contained in the new registration information whenever said new registration information is transmitted, The criteria-of-control preparation method according to claim 5 being a standard which

judges whether it has already existed in a list of said identifiers currently transmitted and held from said two or more data transfer units.

[Claim 7]When a decision result by said judging standard shows that said same identifier exists during said list, consider that all the data request terminal units which have the identifier same in them are inaccurate things, and as said criteria of control, The criteria-of-control preparation method according to claim 6 creating or updating unjust information on a data request terminal unit it was considered that were these inaccurate things.

[Claim 8]a decision result by said judging standard -- (1) -- it considering that all the data request terminal units which have the identifier same in them are inaccurate things, and as said criteria of control, when it is shown that said same identifier exists during said list, Unjust information on a data request terminal unit it was considered that were these inaccurate things is created, or -- updating -- (2) -- it considering that a data request terminal unit which has said identifier contained in said new registration information is a regular thing, and as said criteria of control, when it is shown that said same identifier does not exist during said list, The criteria-of-control preparation method according to claim 6 creating or updating regular information on a data request terminal unit it was considered that was the regular thing.

[Claim 9]Said controlling device transmits to said data transfer unit, and said all or a part of unjust information, or said regular information said data transfer unit, When a data request occurs from each data request terminal unit, about those data requests, The criteria-of-control preparation method according to claim 8 being what determines whether transmit the demanded data to a data request terminal unit which attested using said transmitted unjust information or regular information at least, and performed said data request according to the authentication result.

[Claim 10]When said controlling device transmits said a part of unjust information to said data transfer unit, The criteria-of-control preparation method according to claim 4 or 9 which extracts information corresponding to the data transfer unit and a data request terminal unit in connecting relation among information about a data request terminal unit currently mentioned to said unjust information, and is characterized by transmitting.

[Claim 11]A criteria-of-control preparing system comprising:

Two or more data request terminal units which have a respectively peculiar identifier.

When a data request occurs from these data request terminal unit, about those data requests, performing attestation based on a predetermined attestation standard -- (1) -- to a data request terminal unit which performed said data request according to a result of the attestation, determining whether transmit the demanded data -- (2) -- always -- or according to a result of the attestation with a data transfer unit which outputs data request history information containing said identifier of the data request terminal unit. A controlling device which acquires said outputted data request history information, judges whether a data request terminal unit contained in the data request history information by predetermined judging standard is regular, is based on the decision result, and creates or updates criteria of control.

[Claim 12]A medium recording a program for making a computer perform any of claims 1-10, or all or a part of steps of each steps of one statement.

[Claim 13]A medium recording a program for making a computer perform a function of all or a part of means of each means according to claim 11.

[Translation done.]